MAIL STOP APPEAL BRIEF-PATENTS
PATENTS
2001-1130

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Ralph Rogier DE LA BRETONIERE — Conf. 9140

Application No. 09/509,983 — Group 2155

Filed April 5, 2000 — Examiner M. Young Won

METHOD AND DEVICE FOR
PROTECTING DATA COMMUNICATION

APPEAL BRIEF

MAY IT PLEASE YOUR HONORS: October 17, 2005

(i) **Real Party in Interest**

The real party in interest in this appeal is the appellant/inventor, Ralph Rogier DE LA BRETONIERE.

(ii) **Related Appeals and Interferences**

Neither the appellant nor appellant's legal representative know of any other prior or pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(iii) **Status of the Claims**

Claims 1-20 are pending.

iv) **Status of Amendments**

The claims were last amended in the After Final

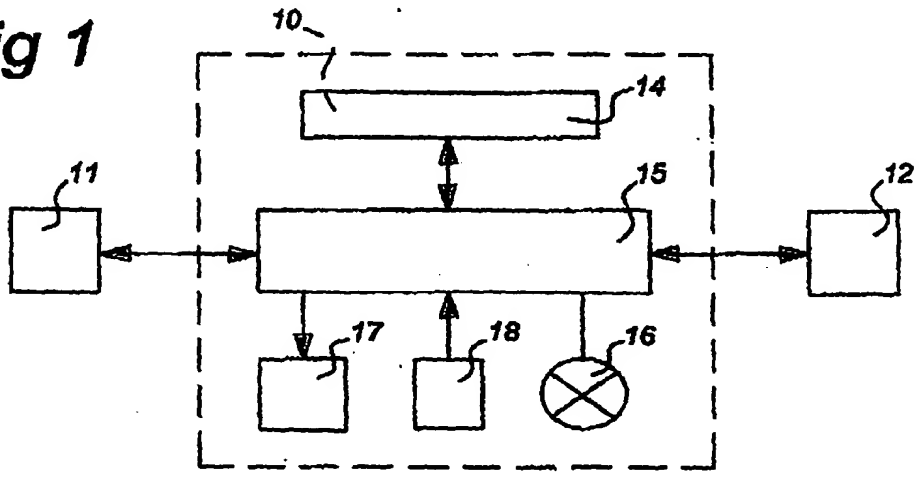
Amendment of June 15, 2005. The Advisory Action of July 26, 2005 indicated that the After Final Amendment would be entered for the purposes of appeal. The claims, as pending, are as set forth in the Claims Appendix.

(v) **Summary of Claimed Subject Matter**

Claims 1, 4, and 10 are independent.

The invention is a protection method and a protection device (Figure 1, 10) between a data receiving first communication station (Figure 1, element 11) and a data sending second communication station (12). See also Background of the Invention (specification page 1, paragraph 1). More specifically, the inventive method and device prevents a third party from being able to make unnoticed use of the receiving first station (11). See specification page 4, second full paragraph under Summary of the Invention.

Fig 1



As shown by Figure 1, the protection device (10) is located intermediate the sending and receiving stations.

The last paragraph of specification page 6 begins detailing the operation and structure of the protection device. A comparison and forwarding module (15) connects the first and second stations, establishing a physical communication link between a first input receiving incoming data from the second station (12) and a second input to send the received data to the first station (11). A memory unit (14), connected to the comparison and forwarding module, stores characteristics of a standardized communication protocol.

The comparison and forwarding module is configured to compare the stored standardized communication protocol to a data protocol of incoming data received at the first input, and

i) to forward the incoming data to the second input when the comparison determines the data protocol conforms with the standardized communications protocol, or

ii) to ***physically open the communication link*** when the comparison determines the data protocol fails to conform with the standardized communications protocol.

Thus, the comparison and forwarding module (15) compares the incoming data protocol with the stored standardized communications protocol to not forward the

incoming data when the data protocol does not comply with the standardized communication protocol. The not forwarding is assured by the comparison and forwarding module ***physically opening the communication link within the protection device*** to prevent communications between the first and second stations.

In this regard, method claim 1 recites "to ***physically open*** the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol" and "not forwarding data of which the data protocol does not comply with the standardized communication protocol from the data communication protection device to the first communication station by ***physically opening*** the communication link within the protection device to prevent communications between the first communication station (11) and the second communication station (12)."

Device claims 4 and 10 each recite "ii) to ***physically open*** the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol."

(vi) **Grounds of Rejection to be Reviewed on Appeal**

Whether the rejection of claims 1, 4, 10-11, 13, 15, 17 and 19-20 under §102(e) as anticipated by GREEN et al. 6,003,084 ("GREEN") was proper.

Whether the rejections were proper, i.e., the rejections of claims 12, 14, 16, and 18 over GREEN; claims 2 and 5 over GREEN in view of AZUMA et al. 6,430,150; claims 3 and 8 over GREEN in view of ENGEL 5,124,984; claim 6 over GREEN in view of BOEBERT et al. 5,864,683 and ENGEL; claim 6 over GREEN in view of BOEBERT et al.; claim 9 over GREEN in view of BARR 4,763,357.

(vii) **Arguments**

The Independent Claims

Simply put, GREEN does not anticipate because GREEN does not disclose a comparison and forwarding module establishing a physical communication link between a first input receiving incoming data from the second station and a second input to send the received data to the first station, the module operable:

"to ***physically open*** the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol",

"not forwarding data of which the data protocol does not comply with the standardized communication protocol from the data communication protection device to the first communication station by ***physically opening*** the communication link within the protection device to prevent communications between the first communication station (11) and the second communication station (12)", or

"ii) to ***physically open*** the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol."

GREEN relates to a secure network proxy for connecting entities, particularly on TCP/IP networks. GREEN teaches software provisions in the OSI model layers 4-7, and does not actually physically disconnect the communicating entities. Moreover, this would be clear to one of skill in the art as physical disconnection of the communicating entities is not possible at all in a TCP/IP network. This is because that in such a case, the complete network would fail, leading to the situation in which no communication is possible at all.

The Examiner's position is stated in the last 3 lines of page 4 of the Final Official Action (February 14, 2005) and the first 7 lines on page 5.

The Examiner asserts that GREEN breaks the communication link between a sending station and a receiving station, and that GREEN does not forward data when the incoming data protocol does not comply with the standardize data protocol "by physically opening the communication link within the protection device." The Examiner offers GREEN column 10, lines 40-61, and column 12, lines 14-19.

Appellant agrees that GREEN discloses cancelling active sessions and closing a connection supporting the

sessions, but GREEN does not disclose breaking a communication link by physically opening the communication link within a protection device.

The passage from column 10, lines 43-57 is reproduced below, the passages referred to by the Official Action being shown in bold:

> **The filter component then processes the BIND and returns status to the communications component. Based on the status, the proxy may pass the BIND on to the X.500 server, or it may cancel both sessions and close the connections.** The status to be returned on error will be configurable.
> Because the proxy does not implement OSI transport, session, presentation, ACSE or ROSE layers, it will have to manually build appropriate responses to reject or even **possibly abort a connection which may be in place.** For example, if the proxy has an established TCP connection and a TP0 connection then receives a presentation P-CONNECT request with an ACSE A-ASSOCIATE request for X.400 presentation context, the proxy must **generate a rejection to this request, and close the connections.**

In the sentence spanning pages 3-4 of the Official Action (April 29, 2003), the Examiner stated that "[i]t is inherent that when connections are closed, the communication links are terminated either physically or electronically and therefore does not patentably distinguish the invention."

However, to anticipate, GREEN must disclose a physically interruption, i.e., physically opening the communications link. GREEN does not disclose a physically interruption by opening the communications link, but teaches a software closing of the active sessions.

As noted, GREEN teaches software provisions in the OSI model layers 4-7 that do not actually physically disconnect the communicating entities, i.e., by physically opening the communications link. Thus, there is no anticipation.

In the last paragraph on page 14 of the Final Official Action, the Examiner responded to appellant's previous arguments as to why GREEN does not make this "physically opens" disclosure, asserting that GREEN at column 10, lines 45-47 makes the disclosure of physically opening.

More specifically, the Examiner stated that "[w]hen Green discloses, 'cancel both sessions and close the connections', one of ordinary skill in the art would conclude that this teaches the limitation because closing the connection results in terminating communication and when communication links are physically opened the communication links can no longer transfer current ('opened circuit') thereby preventing data to be communicated."

This conclusion is incorrect and inconsistent with the position taken in the April, 2003 Official Action.

GREEN does disclose to "cancel both sessions and close the connection." However, there is no basis for concluding the one of ordinary skill would interpret "close the connection" as inherently meaning the communications

circuit is physically opened.

In the Advisory Action (dated July 26, 2005) two new electronic documents are offered to support the Examiner's position. But the Examiner's logic is flawed, which flawed logic renders the rejection flawed and improper.

The Examiner reverses the "how-result" steps which are necessary for one of ordinary skill to reach the desired result of closing the connection. The connection being closed does not ***require*** the physical opening of the communication link. It is flawed reasoning to take the phrase "close the connection" to necessarily mean "open circuit" or "physically open the communication link".

One of ordinary skill, having read and understood the present application, would know that there are plural possibilities to "close the connection" (the genus). Physically opening the connection, as taught by the present application, is one possibility (a species of the genus). But GREEN teaches another possibility and a very different solution, i.e., to logically close the connection (another species of the genus).

In GREEN, to "close the connection", the connection is logically closed; but the physical connection stays in place, and must stay in place in order not to disrupt the complete network.

See again that GREEN at column 10 discloses software actions being taken. At line 43, "The filter component then processes the BIND and returns status to the communications component. Based on the status, the proxy may pass the BIND on to the X.500 server, or it may cancel both sessions and close the connections." This passage includes lines 45-47.

GREEN discloses to "cancel both sessions and close the connections", but the skilled person will not interpret this as physically breaking up the connections, but as logically closing the connection, with the physical connection (electrical wiring) remaining in place, as otherwise, the complete computer network would break down.

Although it is mentioned in GREEN that "...the proxy could be rude and just close the IP connection, but this is really not appropriate..." (column 10, lines 57-58), such a statement in fact teaches away the skilled person from physically opening the connection (as being not appropriate). This is exemplified by the following lines 60-61 in the same paragraph, "The appropriate response would be to build an ACSE A-ASSOCIATE response of 'rejected (permanently)'."

So, GREEN teaches to stop the logical connection (by using the network command "rejected (permanently)"), and not to physically open the associated electrical connection.

Thus, the limitation to "physically open the communication link" is not disclosed by GREEN. Rather, GREEN not only does not anticipate but GREEN teaches away from that recited.

Reversal of the GREEN anticipation rejection is accordingly respectfully requested.

The Dependent Claims

The dependent claims are believed allowable at least for depending from an allowable independent claim.

Conclusion

The GREEN anticipation rejection is improper and therefore reversal of the GREEN anticipation rejection is respectfully requested. Reversal of the obviousness rejections is also respectfully requested.

(viii) **Claims Appendix**

A copy of the claims involved in the appeal.

(ix) **Evidence Appendix**

None.

(x) **Related Proceedings Appendix**

None.

Respectfully submitted,

YOUNG & THOMPSON

Roland E. Long, Jr. Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/lk

(viii) **Claims Appendix**

1. Method for protecting data communication traffic between a first communication station (11) and a second communication station (12), in which the data is dispatched according to a data protocol from the second communication station to the first communication station, comprising the steps of:

(i) receiving the data from the second communication station (12) in a data communication protection device (10),

the protection device having i) a first input for connection to an incoming communication line receiving the data communication from the second communication station, ii) a second input for connection to the first communication station, iii) a comparison and forwarding module connected intermediate the first input and the second input and establishing a physical communication link between the first input and the second input, and iv) a memory connected to the comparison and forwarding module, the memory unit storing characteristics of a standardized communications protocol of first communication device,

the comparison and forwarding module configured to compare the standardized communications protocol to a data protocol of incoming data from the first input, and i) to forward the incoming data to the second input when the

comparison determines the data protocol conforms with the standardized communications protocol and ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol;

(ii) comparing the data protocol of the data with the standardized communication protocol in the data communication protection device (10), characterized by

(iii) forwarding data of which the data protocol complies with the standardized communication protocol from the data communication protection device (10) to the first communication station (11), and not forwarding data of which the data protocol does not comply with the standardized communication protocol from the data communication protection device to the first communication station by physically opening the communication link within the protection device to prevent communications between the first communication station (11) and the second communication station (12).

2. Method according to Claim 1, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a warning is generated.

3. Method according to claim 1, characterized in that, after it has emerged during the comparison of the data

protocol that the latter does not comply with the at least one standardized protocol, a data file containing data of the data communication traffic and the second communication station (12) is stored.

4. Data communication protection device (10) arranged for protecting data communication traffic between a first communication station (1) and a second communication station (12), data being dispatched according to a data protocol from the second communication station to the first communication station, the data communication protection device comprising:

a first input for connection to an incoming communication line receiving the data communication from the second communication station;

a second input for connection to the first communication station;

a comparison and forwarding module connected intermediate the first input and the second input and establishing a physical communication link between the first input and the second input; and

a memory connected to the comparison and forwarding module,

the memory unit storing characteristics of a standardized communications protocol of first communication device,

the comparison and forwarding module configured to compare the standardized communications protocol to a data protocol of incoming data from the first input, and i) to forward the incoming data to the second input when the comparison determines the data protocol conforms with the standardized communications protocol and ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol.

5. Data communication device according to Claim 4, characterized in that the device furthermore comprises warning means (16) linked to the comparison/forwarding means (15) which give a warning after it has emerged during the comparison of the data protocol that it does not belong to the at least one standardized protocol.

6. Device according to Claim 4, characterized in that the device furthermore comprises display means (17) linked to the comparison/forwarding means (15), the display means (17) displaying data relating to the data communication traffic and the second communication station (12), which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

7. Device according to Claim 6, characterized in

that the device furthermore comprises input means (18) linked to the comparison/forwarding means (15) for inputting commands relating to the display of the data.

8. Device according to Claim 4, characterized in that the device comprises interface means for exchanging data relating to the data communication traffic and the second communication station (12) with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

9. Device according to Claim 4, characterized in that the device (10) is integrated in the first communication station (11).

10. A remote diagnostics and protective device, comprising:

a first input for connection to an incoming communication line;

a second input for connection to a communication apparatus;

a comparison and forwarding module connected intermediate the first input and the second input and establishing a physical communication link between the first input and the second input; and

a memory connected to the comparison and forwarding module,

the memory unit storing characteristics of a standardized communication protocol,

the comparison and forwarding module configured to compare the standardized communication protocol to a data protocol of incoming data from the first input, and i) to forward the incoming data to the second input when the comparison determines the data protocol conforms with the standardized communication protocol and ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol.

11. The device of claim 10, wherein when the comparison and forwarding module opens the communication link, a data file of the incoming data is stored in the memory.

12. The device of claim 10, wherein,

the first input is for connection to an incoming telephone line;

the second input is for connection to a telefax machine; and

the memory unit stores characteristics of a standardized protocol of telefax communication,

the comparison and forwarding module is configured to compare the standardized telefax protocol to the data protocol of incoming data from the first input, and i) to forward the incoming data to the second input when the comparison determines the data protocol conforms with the standardized telefax protocol and ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized telefax protocol.

13. The device of claim 12, wherein when the comparison and forwarding module opens the communication link, a data file of the incoming data is stored in the memory.

14. The device of claim 10, wherein,

the first input is for connection to an incoming telephone line;

the second input is for connection to a photocopy machine; and

the memory unit stores characteristics of a standardized protocol of photocopy communication,

the comparison and forwarding module is configured to compare the standardized photocopy protocol to the data protocol of incoming data from the first input, and i) to forward the incoming data to the second input when the

comparison determines the data protocol conforms with the standardized photocopy protocol and ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized photocopy protocol.

15. The device of claim 14, wherein when the comparison and forwarding module opens the communication link, a data file of the incoming data is stored in the memory.

16. The device of claim 10, wherein,

the second input is for connection to a telefax machine; and

the memory unit stores characteristics of a standardized protocol of telefax communication,

the comparison and forwarding module is configured to compare the standardized telefax protocol to the data protocol of incoming data from the first input, and i) to forward the incoming data to the second input when the comparison determines the data protocol conforms with the standardized telefax protocol and ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized telefax protocol.

17. The device of claim 16, wherein when the

comparison and forwarding module opens the communication link, a data file of the incoming data is stored in the memory.

18. The device of claim 10, wherein,

the second input is for connection to a photocopy machine; and

the memory unit stores characteristics of a standardized protocol of photocopy communication,

the comparison and forwarding module is configured to compare the standardized photocopy protocol to the data protocol of incoming data from the first input, and i) to forward the incoming data to the second input when the comparison determines the data protocol conforms with the standardized photocopy protocol and ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized photocopy protocol.

19. The device of claim 18, wherein when the comparison and forwarding module opens the communication link, a data file of the incoming data is stored in the memory.

20. The device of claim 10, wherein the standardized communication protocol is other than a TCP/IP protocol component.